We claim:

1. An integrated networking device comprising:

a first access interface within a plurality of access interfaces, the first interface coupled to a first network and adapted to transmit packets to the first network and receive packets from the first network;

a second access interface within the plurality of access interfaces, the second interface coupled to a second network and adapted to transmit packets to the second network and receive packets from the second network, the second network operating on a different medium than the first network;

a packet processor coupled to the plurality of access interfaces, the packet processor adapted to identify a packet type and provide packet security within the device, the packet processor comprising;

a packet-filtering firewall for isolating and analyzing packets according to their content in order to prevent unauthorized access to an attached network;

a stateful-filtering firewall for isolating and analyze packets according to their state information in order to prevent unauthorized access to an attached network;

a security processor coupled to the packet processor, the security processor adapted to encrypt packets prior to transmission onto the first network and decrypt packets after reception from the first network;

a switching fabric coupled to the plurality of access interfaces, the packet processor, and a plurality of network ports, the switching fabric adapted to transmit packets to a corresponding network port according to a routing protocol within the switching fabric; and

a system processor coupled to the plurality of access interfaces, the switching fabric, the packet processor, and the security processor, the system processor adapted to manage the networking device.

2. The device of claim 1 wherein the first access interfaces couples to a copper-based network.

3. The device of claim 1 wherein the first access interface couples to a fiber optic network.

4. The device of claim 1 wherein the first access interface a transceiver adapted to communicate with a wireless network.

5. The device of claim 1 wherein the packet processor comprises a network address translation module for managing networking policy, configuration, and service for at least one of the attached networks.

6. The device of claim 5 wherein the network address translation module comprises:

an address resolution protocol module for converting an Internet Protocol address to a data link controlled address;

a device configuration table for storing configuration data regarding at least one device on the first network;

a user information table for storing user and customer information.

7. The device of claim 5 wherein the network address translation module dynamically assigns Internet Protocol addresses to at least one device on an attached network.

8. The device of claim 1 wherein the packet processor comprises a box configuration module for storing descriptive data relating to the inter/intra-networking device and corresponding ports.

9. The device of claim 1 wherein the packet processor comprises a security policy database for storing various standards for specifying packet-filtering rules based on information found within a header of a packet.

10. The device of claim 1 wherein the packet processor comprises an anti-virus agent for monitoring at least one connected device on the first network for computer viruses.

11. The device of claim 1 wherein the packet processor comprises an intrusion detection module for inhibiting hacking into the inter/intra-networking device by monitoring packets received by the networking device.

12. The device of claim 1 wherein the packet processor comprises a virtual private network policy and table module for implementing a virtual private network.

13. The device of claim 12 wherein the virtual private network policy and table module comprises:

an Internet Protocol header authentication module for providing connectionless integrity and data origin for Internet Protocol data packets;

an encapsulated security payload module for conveying encrypted data in an Internet Protocol datagram; and

an encryption key module for establishing security associations and cryptographic keys within the first network.

14. The device of claim 1 wherein the packet processor comprises a layer two tunneling module for enabling Internet service providers to operate virtual private networks within the first network.

15. The device of claim 1 wherein the security processor comprises an encryption/decryption module for creating a message for digital signatures corresponding to packets received from the packet processor.

16. The device of claim 15 wherein the encryption/decryption module verifies digital signatures according to the ARCFOUR standard.

17. The device of claim 1 wherein the security processor comprises an internet key exchange module dynamically negotiating security associations and enabling secure communication.

18. The device of claim 1 wherein the security processor comprises an authentication header module for encrypting and decrypting packets according to the authentication header protocols and standards.

19. The device of claim 1 wherein the security processor comprises an encapsulating security payload module for encrypting and decrypting packets according to the encapsulation security payload protocols and standards.

20. The device of claim 1 wherein the routing table is stores routing information for transmitting packets to at least one port within the plurality of ports.

21. The device of claim 1 wherein the switching fabric comprises a switching table that stores switching information for transmitting packets to at least one port within the plurality of ports.

22. The device of claim 1 wherein the system processor comprises a graphical user interface for allowing a network manager to configure and modify network settings on the networking device.

23. The device of claim 1 wherein the system processor comprises a network manager for controlling file transfers between a first device and a second device, the first device operating on the first network.

24. The device of claim 23 wherein the network manager for managing hypertext files in at least one device on the first network.

25. The device of claim 1 wherein the system processor comprises a network management module for managing the first network attached to the networking device.

26. The device of claim 25 wherein the network management module further receives and responds to management information from agents operating on at least one device on the first network according to the Simple Network Protocol.

27. The device of claim 26 wherein management information from agents is stored within a management information database.

28. The device of claim 1 wherein the system processor comprises a routing manager for controlling routing functions performed within the inter/intra-networking device.

29. The device of claim 28 wherein the routing manager supports host address and performs host address translation.

30. The device of claim 29 wherein the routing manager comprises:

an open shortest path first module for determining a path across an attached network according to the Open Shortest Path First Protocol; and

a routing information module for determining a path across an attached network according to the smallest hop count between source and destination.

31. The device of claim 1 wherein the system processor comprises a routing manager for reporting multicast group memberships to any immediately neighboring multicast routing device.

30. The device of claim 1 wherein the system processor comprises a routing manager for supporting multiple quality of service packet characteristics and corresponding internal queues.

31. A method for networking computing devices operating on a plurality of networks operating on different mediums, the method comprising:

receiving a first packet from a first network via a first access interface on a networking device;

receiving a second packet from a second network via a second access interface on a networking device, the second network operating on a different medium than the first network;

identifying a packet type corresponding to the first packet;

applying a packet-filtering firewall to analyze the first packet according to its content in order to prevent unauthorized access to a device on the first network;

applying a stateful-filtering firewall to analyze the first packet according to its state in order to prevent unauthorized access to the device on the first network;

screening the first packet using a network intrusion detection sensor to prevent hacking into the device on the first network;

storing monitoring data regarding the first packet for use in managing the first network;

applying a network address table to convert an incoming port number to a local Internet Protocol or port value; and

switching the first packet to a corresponding network port according to a switching table.

32. The method of claim 31 wherein the step of identifying a packet type further comprises:

identifying whether the first packet is an Internet Protocol security encrypted packet;

decrypting the first packet in order to determine whether there are errors within the first packet;

recover routing information corresponding to the first packet that may have been lost doe to the errors;

determining whether there is an existing virtual connection in a network corresponding to the first packet;

encrypting the first packet; and

transmitting the first packet according to routing information corresponding to the first packet.

33. The method of claim 32 wherein an existing virtual connection is identified by analyzing an authenticated header corresponding to the first packet.

34. The method of claim 32 wherein an existing virtual connection is identified by analyzing an encapsulated security payload corresponding to the first packet.

35. The method of claim 31 wherein the step of identifying a packet-type further comprising:

identifying whether the first packet as a wireless packet;

determining whether the first packet is part of an existing connection that has been previously authorized; and

transmitting packet according to properties of the previously authorized channel.

36. The method of claim 31 further comprising:

creating a configuration table relating to devices on the first network;

maintaining the configuration by analyzing management data within the first packet; and

using the configuration table to manage the first network.

37. The method of claim 31 further comprising:

creating a user information table containing user and customer information relating to at a device on the first network;

maintaining the user information table by analyzing user data within the first packets; and

using the user information table to manage at least one device on the first network.

38. The method of claim 31 further comprising dynamically assigning Internet Protocol addresses to at least one device on the first network.

39. The method of claim 31 further comprising monitoring at least one device on the first network for viruses using an anti-virus agent.

40. The method of claim 31 further comprising configuring port access on the networking device according to a desired security standard.

41. The method of claim 31 further comprising scanning the first packet using an intrusion detection sensor to inhibit hacking into a device on the first network.

42. The method of claim 31 further comprising creating a message for a digital signature corresponding to the first packet.

43. The method of claim 42 further comprising verifying the digital signature according to ARCFOUR standards.

44. The method of claim 31 further comprising controlling file transfers between a first and second device, the first device operating on the first network and the file transfer performed according to the File Transfer Protocol.

45. The method of 31 further comprising creating a Web page stored in a device on the first network.

46. The method of claim 45 further comprising maintaining a Web page stored in a device on the first network.

47. The method of claim 31 further comprising reporting multicast group memberships to any immediately neighboring multicasting routing device.

48. The method of claim 31 further comprising switching the first packet according to quality of service characteristics corresponding to the first packet.